High-Assurance Security/Safety on HPEC Systems: an Oxymoron?

Bill Beckwith
Objective Interface Systems, Inc.
Phone: 703-295-6519
Email Address: bill.beckwith@ois.com

W. Mark Vanfleet
National Security Agency
Phone: 410-854-6361
Email Address: wvanflee@restarea.ncsc.mil

Summary:

To address the need for security in high performance systems, an architecture-based on a small separation, or partitioning, kernel was proposed. This architecture, termed the MILS (Multiple Independent Levels of Security) architecture classifies the components of a system into three layers, the Partitioning Kernel, the Middleware layer (which includes many operating system functions commonly found combined with an OS kernel, as well as code more traditionally termed middleware), and the Application layer. This approach can be implemented and used effectively in high performance systems.

In MILS, basic, general-purpose security policies are enforced at lower levels by the Partitioning Kernel and middleware layer. Enforcement of these basic security policies permits the top layer to implement other, application-specific security policies-such as Bell-LaPadula (BLP), Biba, Community of Interest, etc.-with confidence that the code that implements these policies will have the characteristics of a reference monitor: Non-bypassable, Evaluatable, Always-invoked and Tmper-proof (NEAT). The ability of these systems to transfer data at high speed is not compromised by a MILS design.

These concepts are extended to a collection of MILS nodes called an enclave. The PCS (Partitioning Communication System) provides the high-assurance secure communication between the MILS nodes in the enclave. The PCS was designed with HPEC systems in mind. The PCS includes zero-copy semantics for secure communications.

Like the Partitioning Kernel, the PCS requires formal methods and mathematical models to assure correctness. The presentation will describe the performance impact and optimizations of the PCS on HPEC environments.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 FEB 2005	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
High-Assurance Security/Safety on HPEC Systems: an Oxymoron?	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Objective Interface Systems, Inc.; National Security Agency**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM00001742, HPEC-7 Volume 1, Proceedings of the Eighth Annual High Performance Embedded Computing (HPEC) Workshops, 28-30 September 2004 Volume 1., The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**7**	

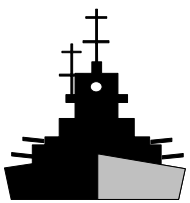
High-Assurance Security/Safety on HPEC Systems: an Oxymoron?

Abstract
Agenda

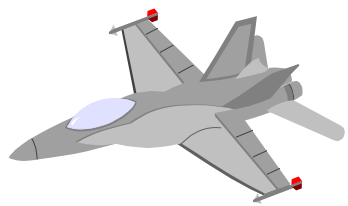
HPEC Poster
30-SEP-2004

W. Mark Vanfleet
Senior NSA/IAD
Security Analyst
wvanflee@restarea.ncsc.mil

Bill Beckwith
Objective Interface Systems
CEO/CTO
bill.beckwith@ois.com



This presentation represents joint research between the
Air Force, Army, Navy, NSA, Boeing, Lockheed Martin, Objective Interface, Green Hills, LynuxWorks, Wind River, GD, Rockwell Collins, MITRE, U of Idaho



The Whole Point of MILS

Really simple:

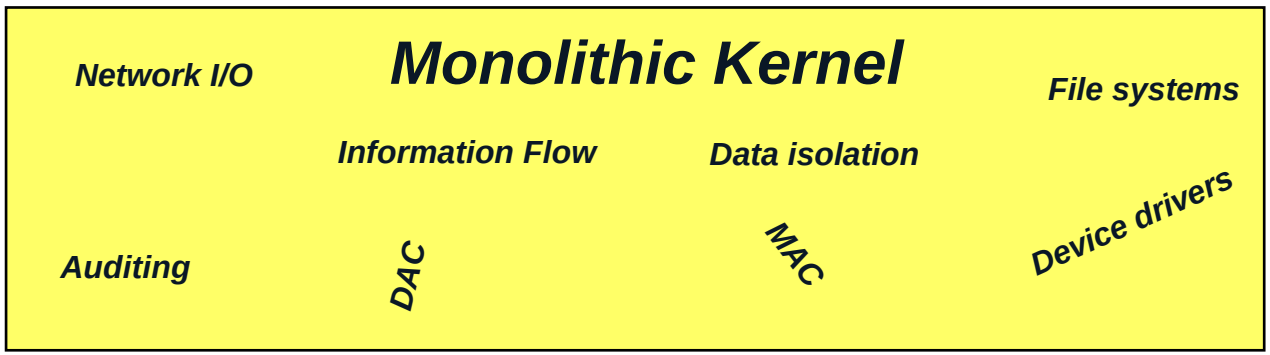
- Dramatically **increase the scrutiny** of *security critical code*
- Dramatically **reduce the amount** of *security critical code*

Orange Book vs. MILS Architecture

User Mode

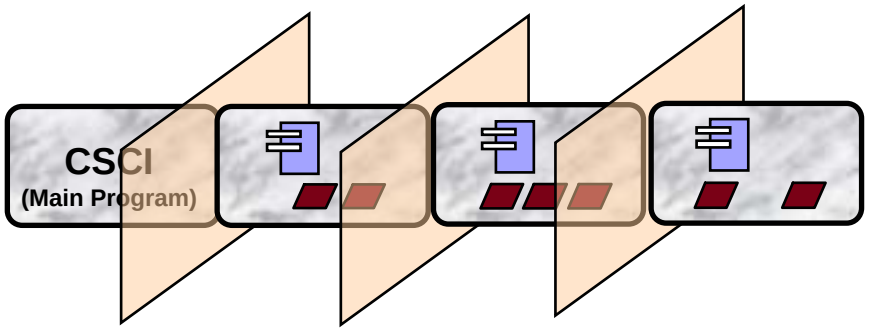
Damage Limitation Periods Processing

Kernel



Privilege Mode

Orange Book vs. MILS Architecture



User Mode

Middleware

Network I/O

File systems

Auditing

DAC

MAC

Device drivers

Mathematical Verification

Partitioning Kernel

Information Flow

Data isolation

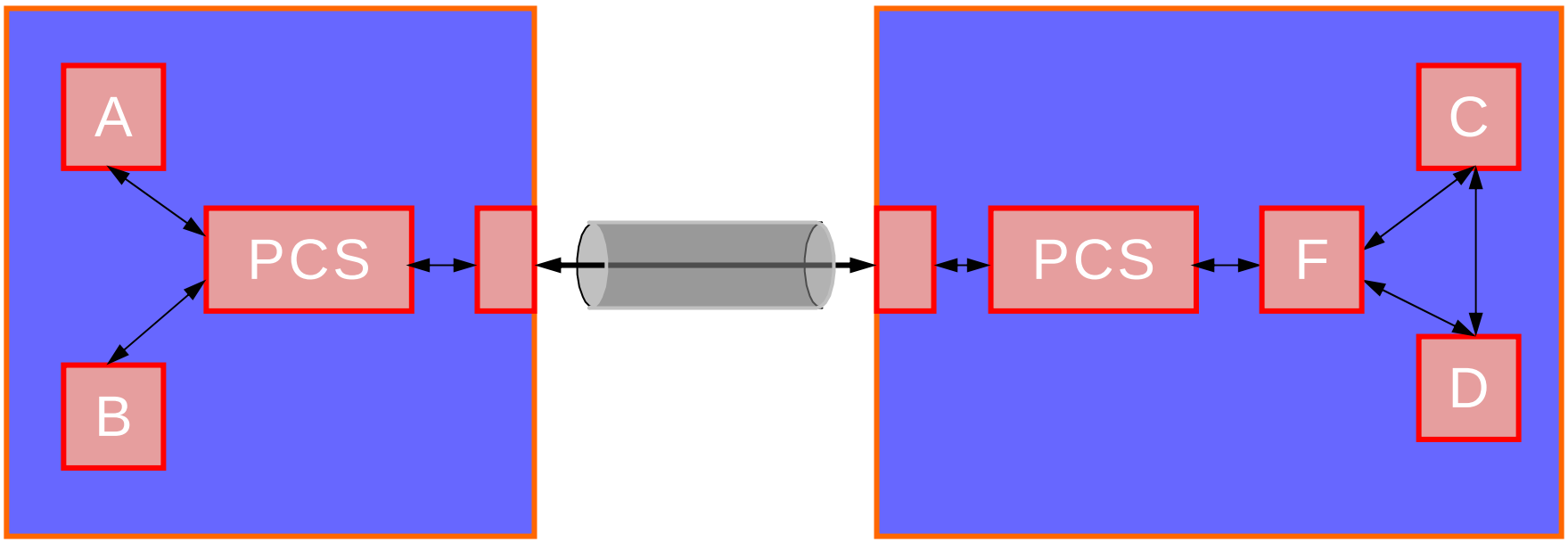
Periods Processing

Damage Limitation

Privilege Mode

Kernel

Zero-copy Secure Communications Channel



Partitioning the Channel